

REMARKS

Claims 1-24 are all the claims pending in the application. The Examiner finally rejects claims 1-4, 9, 10-14, and 21-23 under 35 U.S.C. §103(a) as being unpatentable over Mroczkowski ("Implementation of the block cipher Rijndael using Altera FPGA," May 2000) in view of Luyster (US 6,182,216). The Examiner further rejects claims 5-8 under 35 U.S.C. §103(a) as being unpatentable over Mroczkowski in view of Luyster and further in view of Daemen et al. ("AES Proposal: Rijndael," March 1999).

§ 103(a) Rejection

Claims 1-4, 9, 10-14, and 21-23 are rejected under 35 U.S.C. §103(a) as being unpatentable over Mroczkowski in view of Luyster, and claims 5-8 are rejected under 35 U.S.C. §103(a) as being unpatentable over Mroczkowski in view of Luyster and further in view of Daemen.

To establish a *prima facie* case of obviousness, three basic criteria must be met one of which is that the prior art reference (or references when combined) must teach or suggest all the claim limitations.¹

Claim 1

Regarding independent Claim 1, independent Claim 1 recites an apparatus for encrypting/decrypting a real-time input stream comprising a control unit, a key schedule unit, and a block round unit wherein the control unit receives a data stream of byte units and converts the data stream into block data. *See*, Application, ¶ [0011]. Claim 1 recites "An apparatus ... comprising a control unit ... converting the data stream into block data."

The Examiner states that the control unit receiving a data stream of byte units and converting the data stream into block data was not disclosed in Mroczkowski, and is not explicitly taught in Luyster, but that Luyster inherently teaches converting. Applicants agree that

¹ See, MPEP 2143.

Luyster received a data stream that is already in block form such as 64, 128, or 258 bit blocks as shown in item 50 of Fig. 3. However, Luyster lacks, and does not teach, the structure to convert a stream of byte data into n-bit block data. The Examiner believes this feature is inherent in Luyster. Applicant respectfully disagrees.

Applicant respectfully submits that, even if the structure for converting a stream of data into n-bit data blocks is inherent, this rejection is improper because the principle of inherency may not be used as a basis for rejection under 35 U.S.C. 103(a). *See In re Newell*, 13 U.S.P.Q.2d 1248, 1250 (Fed. Cir. 1989) (The principle of inherency is applicable only with respect to 35 U.S.C. §102 rejections. Inherency and obviousness are distinct concepts. The doctrine of inherency does not extend beyond anticipation.); *see also In re Adams*, 53 CCPA 996, 356 F.2d 998, 148 U.S.P.Q. 742 (1966); *In re Rinehart*, 531 F.2d 1048, 189 U.S.P.Q. 143 (CCPA 1976).

According to MPEP § 2143, the third element necessary for establishing a prima facie case of obviousness is that the prior art reference must teach or suggest all the claim limitations. The Examiner has recognized in the Office Action dated January 12, 2006 that Luyster lacks explicit teachings relating the structure to convert a stream of data into n-bit data blocks (“Luyster does not explicitly teach receiving a stream of byte data, it [is] inherent that data is received streamed.”)². Luyster, Fig. 3, item 50, teaches an n-bit block of data for further processing before encryption wherein n is, for example, 64, 128, or 256 bits. Luyster therefore, receives data already formed into blocks of a specific size rather than teaching the limitation of converting the data stream into block data of claim 1. In addition, the Office Action fails to identify any reference that provides the requisite teaching. Applicant acknowledges that in limited circumstances, it is appropriate for an Examiner to take official notice of facts not in the record or to rely on “common knowledge” in making a rejection. However, MPEP § 2144.03 requires that “such rejections should be judiciously applied.”

In the Office Action made final, examiner gave new grounds of rejection (inherency), which was not necessitated by any amendments made by applicant, thus the final rejection was premature, and. *See* MPEP 706.07(d). Applicant further requests that the Examiner provides a

² *See*, Office Action dated January 12, 2006, page 2, paragraph 1.

reference teaching the limitations missing in Luyster and Mroczkowski, or allow the claim 1 and its dependencies over the cited references because neither Mroczkowski nor Luyster, either separately or in combination, teach all the limitations of Claim 1, and the prima facie case of obviousness fails.

Claim 10

Independent Claim 10, like Claim 1, recites a control unit receiving a real-time data stream in a first format and converting the data stream into a second format. Luyster's block 50 does not convert a stream of data from one format to another format. Block 50 divides the n-bit cipher input that is already present into x round segments, each round segment containing n divided by x bits.³ Luyster is silent regarding the format of the data in block 50 or in the round segments, and does not teach that the format of the data in block 50 is different than the format of the data in the round segments. The limitation of converting the input data from one format to another is missing from Luyster's block 50.

The Examiner has rejected claim 10 on the same grounds as the claim 1 rejection. Applicant respectfully disagrees that the conversion step of claim 10 is inherent in Luyster. Luyster does not teach conversion from a first data format into a second data format, and the Examiner has not provided any reasoning for the assumed inherency.

For the reasons stated in Applicant's analysis of claim 1 and the reasons state above, Applicant respectfully requests that finality be withdrawn, and that the Examiner either allow claim 10 or provide a reference teaching the limitations missing in Luyster and Mroczkowski.

Claim 22

Independent Claim 22 is similar to independent Claim 10 and requires the conversion of a data stream of a first format into a second format. As in the analysis of Claim 10, Luyster does not teach this limitation.

³ See, Luyster, col. 18, lines 54-67.

For the reasons stated in Applicant's analysis of claim 1, Applicant respectfully requests that finality be withdrawn, and that the Examiner either allow claim 22 or provide a reference teaching the limitations missing in Luyster and Mroczkowski.

Claims 2-9, 11-21, and 23-24

Dependent Claims 2-9, 11-21, and 23-24 depend from allowable independent claims 1, 10, and 22 and are therefore also allowable. "If an independent claim is nonobvious under 35 U.S.C. 103, then any claim depending therefrom is nonobvious. In re Fine, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)."⁴

Applicant respectfully asserts that dependent Claims 2-9, 11-21, and 23-24 are allowable as well and requests reconsideration and withdrawal of the rejection.

⁴ See, MPEP 2143.03.

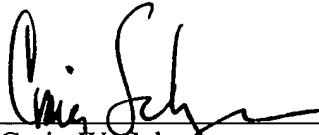
CONCLUSION

In view of the above, withdrawal of finality and reconsideration and allowance of this application are now believed to be in order, and such actions are hereby solicited. If any points remain in issue which the Examiner feels may be best resolved through a personal or telephone interview, the Examiner is kindly invited to contact the undersigned at the telephone number listed below.

Respectfully submitted,
Lee, Hong, Degerman, Kang & Schmadeka

Date: April 11, 2006

By: _____


Craig W. Schmeier
Registration No. 51,007
Attorney for Applicant(s)

Lee, Hong, Degerman, Kang & Schmadeka
801 S. Figueroa Street, 14th Floor
Los Angeles, CA 90012
Telephone: (213) 623-2221
Facsimile: (213) 623-2211